(12) UK Patent Application (19) GB (11) 2 201 125 (13) A

(43) Application published 24 Aug 1988

(21) Application No 8703540

(22) Date of filing 16 Feb 1987

(51) INT CL⁴
G06K 5/00

(52) Domestic classification (Edition J):
B6A C11 C81 C91 K
G4H 13D 14A 1A TG
U1S 2271 B6A G4H

(56) Documents cited
EP 0174016 WO 86/03040 WO 82/03286
US 4529870

(58) Field of search
B6A
G4H

(71) Applicant
De La Rue Systems Limited

(Incorporated in United Kingdom)

De La Rue House, 3/5 Burlington Gardens, London, W1A 1DL

(72) Inventors
Paul Derek Miles
Martin Fogg

(74) Agent and/or Address for Service
Gill Jennings & Every
53/64 Chancery Lane, London, WC2A 1HN

(54) Verification device

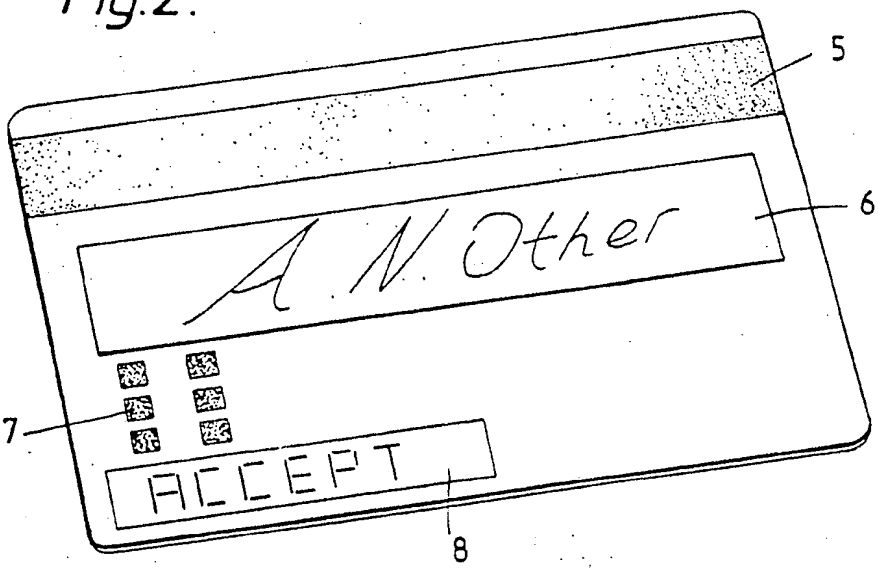
(57) A verification device comprises a body of the size and appearance of a credit card, and having within it processing and storage circuitry, and characterised by having both input means (6) and indication means (8) whereby data can be input and an indication of verification (when the data is correct) can be given.

In a preferred form (Fig 2) the input device is a signature pressure pad, and the indication means displays the word "accept" when the input signature agrees with characteristics stored in the card.

Alternatively the input means may be a keyboard, and the input data may be a PIN code.

Contacts 7 allow data transfer with an external device (e.g. a cash dispenser) whereby a signal can be output to the external device as a result of verification of data input direct to the card.

Fig.2.



The drawing(s) originally filed was (were) informal and the print here reproduced is taken from a later filed formal copy.

GB 2 201 125 A

2201125

Fig.1.

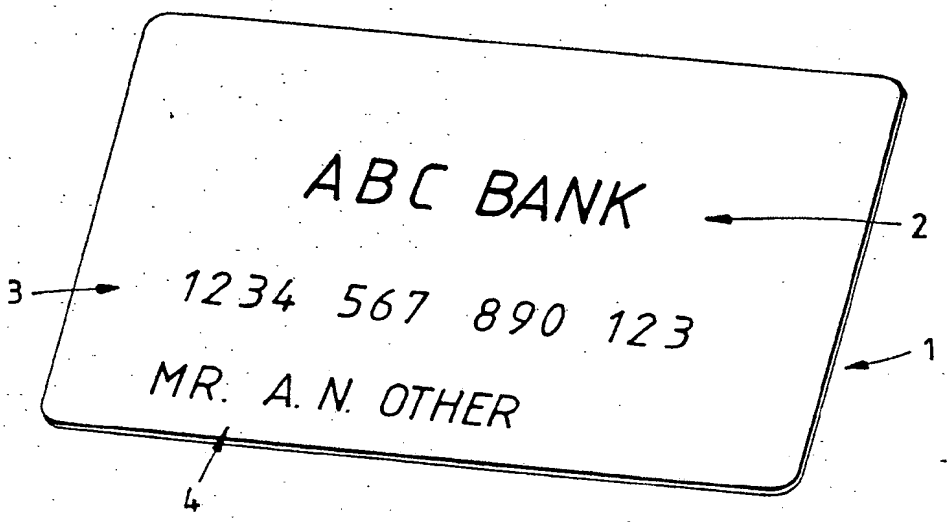
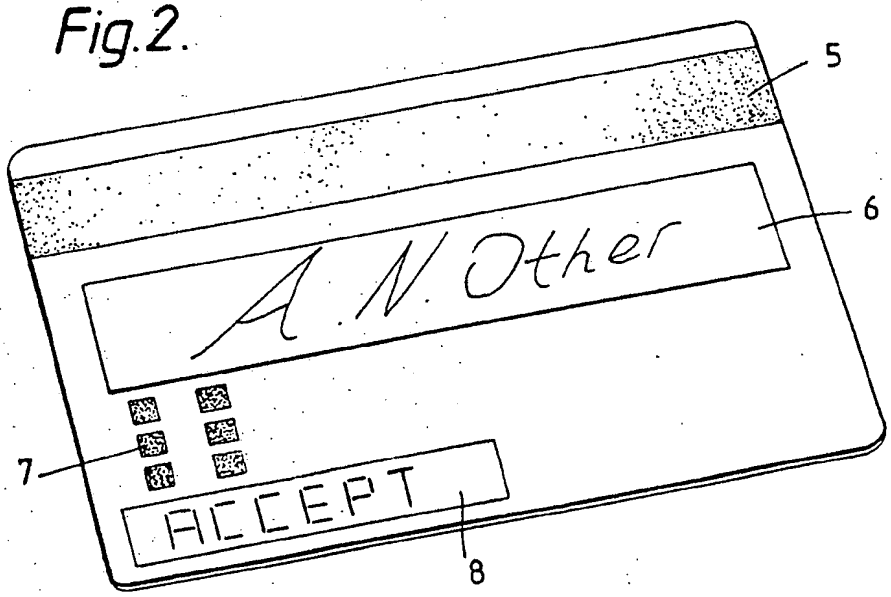
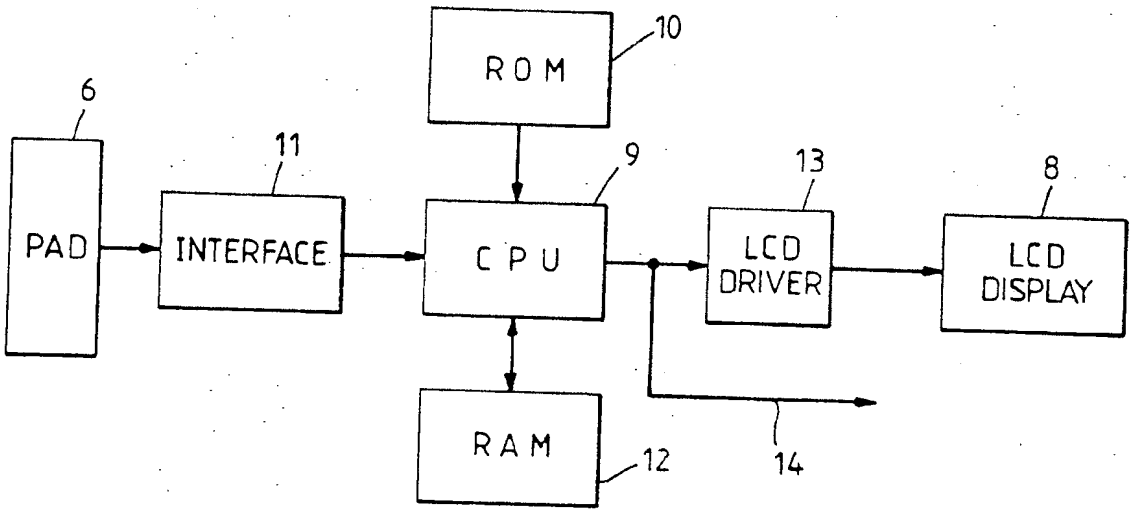


Fig.2.



2201125

Fig.3.



MW
M Sigmaduine

2201125

VERIFICATION DEVICE

The invention relates to verification devices, for example of the type for verifying signatures.

Conventional signature verification devices comprise wall mounted systems to which a user must go to enable his signature to be verified. Typically, the user identifies himself, for example by keying in a personal identification number or the like or by inserting a credit card like article from which his details are read. The user then signs his name on a pressure pad and the written signature is analysed to determine certain characteristics of the signature and these characteristics are then compared with previously stored characteristics indicative of that user. If the comparisons are satisfactory, the signature is verified and the user can then access the facility provided by the system. This may be, for example, a cash dispenser to enable the user to draw out a certain quantity of banknotes or a door control device enabling the user to gain access to a particular area.

One of the problems with these known devices is the need to provide complex wall mounted verification systems in association with each cash dispenser or other equipment to be actuated when a signature is verified. A further problem in the case where characteristic details of the bearer's signature are already stored on a credit card like article is that it is possible to derive the information relating to that signature as it is passed from the card to the verification system to enable the written signature to be verified.

In accordance with the present invention, we provide a self-contained verification device comprising a card-like article in which is embodied a memory, a processor, and input means, the processor being

responsive to information received from the input means to verify that information by reference to information previously stored in the memory and to generate a signal representative of the result of the verification.

The invention provides a convenient device which carries out the verification process internally without any information being passed between a remote system and the card-like article. Thus, the user enters the necessary information via the input means, this information being fed to the processor which then compares the information with the previously stored information in the memory. If the comparison is successful, and the information input is verified, a signal indicative of that fact is output. If the comparison is unsuccessful and the signature is not verified then a different signal is generated.

The information may be verified by the processor by direct comparison with information in the memory, for example in the case where the input means comprises a key pad and the information is numeric or alphanumeric data. In other examples secondary information may have been derived from the input information which is compared with the stored information, for example, in the case where the input means comprises a pressure pad on which a signature is written. In this latter case, the processor may derive certain information characteristic of that signature in a known manner.

Preferably, the information which is stored in the memory is substantially unique to the bearer of the card-like article.

In some examples, the signal which is generated may be passed directly to the equipment which requires the verification information. Conveniently, this signal represents the result of the comparison in an encrypted form. In other examples, the device may also embody

display means responsive to the signal representative of the result of the comparison to provide a visual indication of the result of the verification. This display means may comprise an LCD display or the like.

In its simplest form, the memory in the device may store a PIN or the like and the processor may be programmed to verify an input PIN with the stored PIN and, under certain conditions, may permit the stored PIN to be changed. In other cases, the processor may also enable the stored information to be changed when, for example, a particular code is entered.

A further advantage of this device is that it is portable and may be carried by the user and the information stored in the memory may, if the processor is suitably programmed, be changed at the user's leisure in his home for example and without any reference to external equipment.

In order that the invention may be better understood, an embodiment of a self-contained verification device according to the invention will now be described with reference to the accompanying drawings, in which:-

Figure 1 is a plan of one side of the device;

Figure 2 is a plan of the other side of the device; and,

Figure 3 is a block circuit diagram of the elements contained within the device.

The card-like article 1 shown in the drawings may comprise a modified form of "smart" card as manufactured by Casio or Bull and have a "credit card" size. The front face of the card 1 may be printed with conventional information such as the name of issuing institution 2, a card number 3, and the name of the bearer 4.

The reverse side of the card 1 carries a conventional magnetic stripe 5. In addition, a pressure

pad made from a thin piezoelectric film 6 is embodied in the card. An array of electrical contacts 7 is positioned below the pressure pad 6 and an LCD display 8 is embodied in the card below the contacts 7.

Within the card 1 are positioned a number of integrated circuits embodied in a conventional manner on a silicon substrate. These circuits include a microprocessor (CPU) 9 (Figure 3) connected to a read-only memory (ROM) 10 which contains the controlling programme for the microprocessor 9. The pressure pad 6 is connected via conventional interface electronics 11 to the CPU 9. In addition, the CPU 9 is connected to a random access memory (RAM) 12 in which is stored information unique to the bearer of the card such as a PIN or signature data.

The CPU 9 controls the LCD display 8 via an LCD driver 13 to which it is connected.

It will be appreciated that this system is particularly secure because there is no external communications interface between the card and a remote verification device. The internal communication paths will be in the silicon circuits themselves and consequently be very difficult to interfere with to carry out fraudulent transactions. The only external connection is provided by a path 14 connected to the contacts 7 so that a signal indicating whether or not the input signature has been verified can be passed to external equipment such as a cash dispenser to enable operation of this dispenser.

In a typical system, the card 1 is supplied initially to a user with a PIN stored already in the RAM 12. In the comfort of the user's home, he can then activate an enrolment sequence controlled by the CPU 9 in response to a program stored in the ROM 10 to enter firstly the correct PIN. If this entered PIN is

verified with the stored PIN by the CPU 9, the CPU 9 controls the LCD display 8 to display the word "accept" as shown in Figure 2.

The user then signs a number of signatures on the pad 6 (usually between 6 and 9) and the CPU 9 then analyses each signature to derive certain information characteristic of the signature. This information may include pen down time, number of pen lift-offs, and the like as in conventional signature verification techniques. A reference set of signature characteristics is derived from the signatures written and these references are stored in the RAM 12. At this point, the original PIN can be erased from the memory so that the card is only operable in response to a correct signature being entered. In a typical operation, when the user wishes to undertake a financial transaction, the user would sign his name on the pressure pad 6 on the card and the same characteristic information relating to that signature would be derived by the CPU 9 and compared with the reference characteristics stored in the RAM 12. If verification was achieved, the CPU 9 would control the LCD driver 13 to cause the display 8 to display the word "accept" with a corresponding signal being passed along the path 14 to the contacts 7. If the card is placed in a suitable card reader of the cash dispenser, the signal on the path 14 will then cause the cash dispenser to operate.

In an alternative arrangement, the card could be used in a stand alone operation where it is signed in the presence of an equipment operator, a shopkeeper or the like who looks at the indication provided on the display 8 to decide on whether or not the signature is verified. In this case, the path 14 would be omitted.

CLAIMS

1. A self-contained verification device comprising a card-like article in which is embodied a memory, a processor, and input means, the processor being responsive to information received from the input means to verify that information by reference to information previously stored in the memory and to generate a signal representative of the result of the verification.

2. A device according to claim 1, wherein the input means comprises a pressure pad, the processor being adapted to derive information characteristic of a signature written on the pressure pad.

3. A device according to claim 1 or claim 2, further comprising display means embodied in the card-like article connected to the processor to generate a visual indication of the result of the verification.

4. A device according to any of the preceding claims, wherein the memory is adapted to store information substantially unique to the bearer of the article.

5. A self-contained verification device substantially as hereinbefore described with reference to the accompanying drawings.